What is claimed is:

1. A data encryption method, the method including the following steps:

Step A: constructing a security class database for storing a plurality of entries of records of data, each of the entries of records including a data attribute description field and a corresponding encryption definition field, the encryption definition field including a plurality of encryption algorithm module indicators;

Step B: inputting digital data to be encrypted;

Step C: from the security class database, finding a data attribute description that matches attribute of the digital data, and retrieving the corresponding encryption definition data;

Step D: from the retrieved encryption definition data, selecting at random an encryption algorithm module indicator;

Step E: with the selected encryption algorithm module indicator as a guide, controlling encryption processing of the inputted digital data; and

Step F: appending decryption information to the digital data that has undergone encryption processing for subsequent output.

2. The method as claimed in Claim 1, wherein the encryption definition field in the security class database constructed in step A includes a plurality of encryption algorithm module indicators and corresponding proportions adopted thereby, an encryption algorithm module indicator being selected from the retrieved encryption definition data in step D according to each of the encryption algorithm module indicators and the corresponding proportions adopted thereby in cooperation with a random number generator and a MOD operation.

3. The method as claimed in Claim 1, wherein the encryption definition field in the security class database constructed in step A includes a plurality of encryption algorithm module combinations, each of the encryption algorithm

module combinations containing an encryption algorithm module indicator and an authentication algorithm module indicator, an encryption algorithm module combination being retrieved at random from the retrieved encryption definition data in step D, the selected encryption algorithm module combination being used as a guide for controlling encryption processing, including the type of encryption and the type of authentication, of the inputted digital data in step E.

4. The method as claimed in Claim 3, wherein the encryption definition field in the security class database constructed in step A includes a plurality of encryption algorithm module combinations and corresponding proportions adopted thereby, an encryption algorithm module combination being selected from the retrieved encryption definition data in step D according to each of the encryption algorithm module combinations and the corresponding proportions adopted thereby in cooperation with a random number generator and a MOD operation.

5. A data encryption method, the method comprising the following steps:

Step A: constructing an encryption module database for storing a plurality of entries of records of data, each of the entries of records containing an encryption algorithm module indicator and an authentication algorithm module indicator;

Step B: constructing a security class database for storing a plurality of entries of records of data, each of the entries of records containing a data attribute description field and a corresponding encryption definition field, the encryption definition field including a plurality of encryption module database indexes;

Step C: inputting digital data to be encrypted;

Step D: from the security class database, finding a data attribute description that matches attribute of the digital data, and retrieving the corresponding encryption definition data;

Step E: from the retrieved encryption definition data, selecting at random an encryption module database index;

Step F: according to the retrieved encryption module database index, selecting an entry of record from the encryption module database;

Step G: with the selected entry of record as a guide, controlling encryption processing, including the type of encryption and the type of authentication, of the inputted digital data; and

Step H: appending decryption information to the digital data that has undergone encryption processing for subsequent output.

6. The method as claimed in Claim 5, wherein the encryption definition field in the security class database constructed in step B includes a plurality of encryption module database indexes and corresponding proportions adopted thereby, an encryption module database index being selected from the retrieved encryption definition data in step E according to each of the encryption module database indexes and the corresponding proportions adopted thereby in cooperation with a random number generator and a MOD operation.

7. A data encryption method, the method comprising the following steps:

Step A: constructing encryption definition data containing a plurality of encryption algorithm module indicators;

Step B: inputting digital data to be encrypted;

Step C: from the encryption definition data, selecting at random an encryption algorithm module indicator;

Step D: with the selected encryption algorithm module indicator as a guide, controlling encryption processing of the inputted digital data; and

Step E: appending decryption information to the digital data that has undergone encryption processing for subsequent output.

8. The method as claimed in Claim 7, wherein the encryption definition

data constructed in step A includes a plurality of encryption algorithm module indicators and corresponding proportions adopted thereby, an encryption algorithm module indicator being selected from the encryption definition data in step C according to each of the encryption algorithm module indicators and the corresponding proportions adopted thereby in cooperation with a random number generator and a MOD operation.

9. The method as claimed in Claim 7, wherein the encryption definition data constructed in step A includes a plurality of encryption algorithm module combinations, each of the encryption algorithm module combinations including an encryption algorithm module indicator and an authentication algorithm module indicator, an encryption algorithm module combination being selected at random from the retrieved encryption definition data in step C, the selected encryption algorithm module combination being used as a guide for controlling encryption processing, including the type of encryption and the type of authentication, of the inputted digital data in step D.

10. The method as claimed in Claim 9, wherein the encryption definition data constructed in step A includes a plurality of encryption algorithm module combinations and corresponding proportions adopted thereby, an encryption algorithm module combination being selected from the retrieved encryption definition data in step C according to each of the encryption algorithm module combinations and the corresponding proportions adopted thereby in cooperation with a random number generator and a MOD operation.

11. A data encryption method, the method comprising the following steps:

Step A: constructing an encryption module database for storing a plurality of entries of records of data, each of the entries of records containing an encryption algorithm module indicator and an authentication algorithm module indicator;

Step B: constructing encryption definition data which includes a plurality of encryption module database indexes;

Step C: inputting digital data to be encrypted;

Step D: from the encryption definition data, selecting at random an encryption module database index;

Step E: according to the retrieved encryption module database index, selecting an entry of record from the encryption module database;

Step F: with the selected entry of record as a guide, controlling encryption processing, including the type of encryption and the type of authentication, of the inputted digital data; and

Step G: appending decryption information to the digital data that has undergone encryption for subsequent output.

12. The method as claimed in Claim 11, wherein the encryption definition data constructed in step B includes a plurality of encryption module database indexes and corresponding proportions adopted thereby, an encryption module database index being selected from the encryption definition data in step D according to each of the encryption module database indexes and the corresponding proportions adopted thereby in cooperation with a random number generator and a MOD operation.

13. A data encryption method, the method comprising the following steps:

Step A: constructing a security class database for storing a plurality of entries of records of data, each of the entries of records containing a data attribute description field and a corresponding encryption definition field, the encryption definition data field being an encryption algorithm module indicator;

Step B: inputting digital data to be encrypted;

Step C: from the security class database, finding a data attribute description that matches attribute of the digital data, and retrieving the encryption algorithm module indicator of the corresponding encryption definition

field;

Step D: with the selected encryption algorithm module indicator as a guide, controlling encryption processing of the inputted digital data; and

Step E: appending decryption information to the digital data that has undergone encryption processing for subsequent output.

14. The method as claimed in Claim 13, wherein the encryption definition field in the security class database constructed in step A is an encryption algorithm module combination, the encryption algorithm module combination including an encryption algorithm module indicator and an authentication algorithm module indicator, data of an encryption algorithm module combination of the corresponding encryption definition field being retrieved in the step C of finding from the security class database the data attribute description that matches the attribute of the digital data, the selected encryption algorithm module combination being used in step D as a guide for controlling encryption processing, including the type of encryption and the type of authentication, of the inputted digital data.

15. A data encryption method, the method including the following steps:

Step A: constructing an encryption module database for storing a plurality of entries of records of data, each of the entries of records containing an encryption algorithm module indicator and an authentication algorithm module indicator;

Step B: constructing a security class database for storing a plurality of entries of records of data, each of the entries of records containing a data attribute description field and a corresponding encryption definition field, the encryption definition data field being an encryption module database index;

Step C: inputting digital data to be encrypted;

Step D: from the security class database, finding a data attribute description that matches attribute of the digital data, and retrieving the

encryption module database index from the corresponding encryption definition field;

Step E: with the retrieved encryption module database index as a guide, selecting an entry of record from the encryption module database;

Step F: with the selected entry of record as a guide, controlling encryption processing, including the type of encryption and the type of authentication, of the inputted digital data; and

Step G: appending decryption information to the digital data that has undergone encryption processing for subsequent output.

16. A data encryption apparatus, the apparatus having an input portion for input of data and an output portion for output of data after encryption processing thereof, the apparatus further comprising:

a security class database for storing a plurality of entries of records of data, each of the entries of records containing a data attribute description field and a corresponding encryption definition field, the encryption definition field including a plurality of encryption algorithm module indicators;

an inspecting portion for inspecting and separating the data inputted via the input portion into parameter data or digital data;

a parameter processing portion for updating the security class database with the parameter data sent from the inspecting portion;

an attribute inspecting portion for finding from the security class database a data attribute description that matches attribute of the digital data sent from the inspecting portion and for transmitting the corresponding encryption definition data to a encryption selecting portion;

the encryption selecting portion, which selects at random an encryption algorithm module indicator from the retrieved encryption definition data; and

an encryption processing portion for controlling encryption processing of the inputted digital data using the encryption algorithm module indicator selected by the encryption selecting portion as a guide.

17. The apparatus as claimed in Claim 16, wherein the encryption definition field in the security class database includes a plurality of encryption algorithm module indicators and corresponding proportions adopted thereby, the encryption selecting portion selecting an encryption algorithm module indicator from the retrieved encryption definition data according to each of the encryption algorithm module indicators and the corresponding proportions adopted thereby in cooperation with a random number generator and a MOD operation.

18. The apparatus as claimed in Claim 16, wherein the encryption definition field in the security class database includes a plurality of encryption algorithm module combinations, each of the encryption algorithm module combinations including an encryption algorithm module indicator and an authentication algorithm module indicator, the encryption selecting portion selecting at random an encryption algorithm module combination from the retrieved encryption definition data, the encryption processing portion, using the encryption algorithm module combination selected by the encryption selecting portion as a guide, controlling encryption processing, including the type of encryption and the type of authentication, of the inputted digital data.

19. The apparatus as claimed in Claim 18, wherein the encryption definition field in the security class database includes a plurality of encryption algorithm module combinations and corresponding proportions adopted thereby, the encryption selecting portion selecting an encryption algorithm module combination from the retrieved encryption definition data according to each of the encryption algorithm module combinations and the corresponding proportions adopted thereby in cooperation with a random number generator and a MOD operation.

20. The apparatus as claimed in Claim 16, further comprising:
an encryption module database for storing a plurality of entries of records of data, each of the entries of records containing an encryption algorithm module indicator and an authentication algorithm module indicator;
the encryption definition field of the security class database including a plurality of encryption module database indexes;
the encryption selecting portion selecting at random an encryption module database index from the retrieved encryption definition data and, according to the retrieved encryption module database index, and selecting an entry of record from the encryption module database;
the encryption processing portion using the entry of record selected by the encryption selecting portion as a guide to control encryption processing, including the type of encryption and the type of authentication, of the inputted digital data.

21. The apparatus as claimed in Claim 20, wherein the encryption definition field in the security class database includes a plurality of encryption module database indexes and corresponding proportions adopted thereby, the encryption selecting portion selecting an encryption module database index from the retrieved encryption definition data according to each of the encryption module database indexes and the corresponding proportions adopted thereby in cooperation with a random number generator and a MOD operation, and selecting an entry of record from the encryption module database according to the retrieved encryption module database index.

22. The apparatus as claimed in Claim 20, wherein the parameter processing portion updates the security class database and the encryption module database using the parameter data sent from the inspecting portion.

23. A data encryption apparatus, the apparatus having an input portion for

input of data and an output portion for output of data after encryption processing thereof, the apparatus further comprising:

a encryption module database for storing a plurality of entries of records of data, each of the entries of records containing an encryption algorithm module indicator;

an inspecting portion for inspecting and separating the data inputted via the input portion into parameter data or digital data;

a parameter processing portion for updating the encryption module database using the parameter data from the inspecting portion;

a encryption selecting portion for selecting at random an entry of record from the encryption module database; and

an encryption processing portion for controlling encryption processing of the inputted digital data using the entry of record selected by the encryption selecting portion as a guide.

24. The apparatus as claimed in Claim 23, wherein the encryption module database stores a plurality of entries of records of data, each of the entries of records containing an encryption algorithm module indicator and a corresponding proportion adopted thereby, the encryption selecting portion selecting an entry of record according to the corresponding proportion adopted by each of the entries of records in the encryption module database in cooperation with a random number generator and a MOD operation.

25. The apparatus as claimed in Claim 23, wherein the encryption module database stores a plurality of entries of records of data, each of the entries of records containing an encryption algorithm module indicator and an authentication algorithm module indicator, the encryption processing portion controlling encryption processing, including the type of encryption and the type of authentication, using an encryption algorithm module combination of the entry of record selected at random by the encryption selecting portion as a

guide.

26. The apparatus as claimed in Claim 25, wherein the encryption module database stores a plurality of entries of records of data, each of the entries of records containing an encryption algorithm module indicator, an authentication algorithm module indicator and corresponding proportions adopted thereby, the encryption selecting portion selecting an entry of record from the encryption module database according to the corresponding proportion adopted by each entry of record in the encryption module database in cooperation with a random number generator and a MOD operation.

27. A data encryption apparatus, the apparatus having an input portion for input of data and an output portion for output of data after encryption processing thereof, the apparatus further comprising:

a security class database for storing a plurality of entries of records of data, each of the entries of records containing a data attribute description field and a corresponding encryption definition field, the encryption definition field being an encryption algorithm module indicator;

an inspecting portion for inspecting and separating the data inputted via the input portion into parameter data or digital data;

a parameter processing portion for updating the security class database with the parameter data from the inspecting portion;

an attribute inspecting portion for finding from the security class database a data attribute description that matches attribute of the digital data sent from the inspecting portion and for transmitting the corresponding encryption definition data to an encryption processing portion; and

the encryption processing portion for controlling encryption processing of the inputted digital data using the encryption algorithm module indicator selected by the attribute inspecting portion as a guide.

28. The apparatus as claimed in Claim 27, wherein the encryption definition field in the security class database is an encryption algorithm module combination, the encryption algorithm module combination including an encryption algorithm module indicator and an authentication algorithm module indicator, the encryption processing portion, using the encryption algorithm module combination selected by the parameter inspecting portion as a guide, controlling encryption processing, including the type of encryption and the type of authentication, of the inputted digital data.

29. A data decryption method, the method comprising the following steps:

Step A: inputting digital data to be decrypted;

Step B: inspecting whether the digital data includes a decryption algorithm module indicator and, in the affirmative, retrieving the decryption algorithm module indicator or, in the negative, setting the data to be decrypted as equivalent to inputted data for subsequent processing in step D;

Step C: with the retrieved decryption algorithm module indicator as a guide, controlling decryption processing of the inputted digital data; and

Step D: outputting the digital data that has undergone decryption.

30. The method as claimed in Claim 29, wherein, in step B, the digital data is inspected to determine whether the digital data includes a decryption algorithm module combination having a decryption algorithm module indicator and an authentication algorithm module indicator and, in the affirmative, the decryption algorithm module combination is retrieved or, in the negative, the data to be decrypted is set to be equivalent to inputted data for subsequent processing in step D; and in step C, decryption processing, including the type of decryption and the type of authentication, of the inputted digital data is controlled using the selected decryption algorithm module combination as a guide.

31. A data decryption method, the method comprising the following steps:

Step A: constructing a decryption module database for storing a plurality of entries of records of data, each of the entries of records being a decryption algorithm module indicator;

Step B: inputting digital data to be decrypted;

Step C: inspecting whether the digital data includes a decryption module database index and, in the affirmative, retrieving the decryption module database index or, in the negative, setting the data to be decrypted as equivalent to inputted data for subsequent processing in step F;

Step D: with the retrieved decryption module database index as a guide, selecting an entry of record from the decryption module database;

Step E: with the selected entry of record as a guide, controlling decryption processing of the inputted digital data; and

Step F: outputting the digital data that has undergone decryption.

32. The method as claimed in Claim 31, wherein, in step A, a decryption module database for storing a plurality of entries of records of data is constructed, each of the entries of records containing a decryption algorithm module indicator and an authentication algorithm module indicator, and in step E, the selected entry of record is used as a guide for controlling decryption processing, including the type of decryption and the type of authentication, of the inputted digital data.

33. A data decryption apparatus, the apparatus having an input portion for input of data and an output portion for output of data after decryption processing thereof, the apparatus further comprising:

an inspecting portion for inspecting whether the data inputted via the input portion includes a decryption algorithm module indicator and, in the affirmative, retrieving the decryption algorithm module indicator or, in the negative, transmitting the inputted data directly to the output portion; and

a decryption processing portion for controlling decryption processing of the inputted digital data using the decryption algorithm module indicator retrieved by the inspecting portion as a guide.

34. The apparatus as claimed in Claim 33, wherein the inspecting portion inspects whether the data inputted via the input portion includes a decryption algorithm module combination, the decryption algorithm module combination including a decryption algorithm module indicator and an authentication algorithm module indicator, and, in the affirmative, retrieves the decryption algorithm module combination or, in the negative, transmitting directly the inputted data to the output portion, the decryption processing portion controlling the decryption processing, including the type of decryption and the type of authentication, of the inputted digital data using the decryption algorithm module indicator retrieved by the inspecting portion as a guide.

35. The apparatus as claimed in Claim 33, further comprising: a decryption module database for storing a plurality of entries of records of data, each of the entries of records containing a decryption algorithm module indicator, the inspecting portion inspecting whether the data inputted via the input portion includes a decryption module database index and, in the affirmative, retrieving the decryption module database index and further retrieving an entry of record from the decryption module database using the index or, in the negative, transmitting directly the inputted data to the output portion, the decryption processing portion controlling the decryption processing of the inputted digital data using the entry of record retrieved by the inspecting portion as a guide.

36. The apparatus as claimed in Claim 35, wherein the decryption module database stores a plurality of entries of records of data, each of the entries of records containing a decryption algorithm module indicator and an authentication algorithm module indicator, the decryption processing portion

controlling decryption processing, including the type of decryption and the type of authentication, using the entry of record retrieved by the inspecting portion as a guide.

37. The apparatus as claimed in Claim 35, further comprising: a parameter processing portion for updating the decryption module database using parameter data, the inspecting portion inspecting and separating the data inputted via the input portion into parameter data or digital data and, if the inputted data is parameter data, transmitting the same to the parameter processing portion and, if the inputted data is digital data, inspecting whether the digital data includes a decryption module database index and, in the affirmative, retrieving the decryption module database index and further retrieving an entry of record from the decryption module database using the index and, in the negative, transmitting directly the inputted data to the output portion.

38. The apparatus as claimed in Claim 37, wherein the decryption module database stores a plurality of entries of records of data, each of the entries of records containing a decryption algorithm module indicator and an authentication algorithm module indicator, the decryption processing portion controlling decryption processing, including the type of decryption and the type of authentication, of the inputted digital data using the entry of record retrieved by the inspecting portion as a guide.

39. The apparatus as claimed in Claim 21, wherein the parameter processing portion updates the security class database and the encryption module database using the parameter data sent from the inspecting portion.